La sûreté économique comme stratégie de contre intelligence économique

Laurice ALEXANDRE-LECLAIR
alexandr@univ-lyon3.fr

Centre de Recherche de l'IAE, Université Jean Moulin Lyon 3
15, quai Claude Bernard, 69007 Lyon- France.

Mots clés :
intelligence économique, information, sûreté économique, protection, outils.

Key words :
competitive intelligence, data, economic security, protection, instruments.

Palabras Claves :
competitiva inteligencia, informacìon, económica seguridad, protección, instrumentos.

Résumé

L'intelligence économique est la recherche et l'interprétation systématique de l'information accessible à tous, dans un objectif de connaissance des intentions et des capacités des acteurs. Elle englobe toutes les opérations de surveillance de l'environnement concurrentiel (protection, veille, influence) [19]. C'est une démarche organisée, au service du management stratégique de l'entreprise visant à améliorer sa compétitivité par la collecte, le traitement d'informations et la diffusion de connaissances utiles à la maîtrise de son environnement (menaces et opportunités) : ce processus d'aide à la décision utilise des outils spécifiques, mobilise les salariés, et s'appuie sur l'animation de réseaux internes et externes [7]. Les pratiques d'intelligence économique sont aussi bien défensives qu'offensives. Cet article insiste sur l'aspect offensif de l'intelligence économique, et démontre qu'elle peut être aussi dangereuse que l'espionnage industriel. La pratique des techniques de contre-intelligence économique (ou sûreté) s'impose alors au sein des entreprises. L'information semble être dans ce cas, l'arme et le bouclier de cette guerre économique qui se veut surtout une guerre d'information. Il existe alors plusieurs outils de protection de l'information. Ces outils peuvent être de nature juridique ou technique. Ils peuvent être aussi bien au niveau individuel qu'au niveau général de l'entreprise. Ces outils se résument par des clauses de confidentialité ou de non-concurrence, des titres de propriété tel que les brevets par exemple sur le plan juridique. Sur le plan technique, nous évoquons la classifiaction de l'information ou la cryptologie, mais aussi tous les codes d'accès informatique ou autres adoptés à ce jour au sein des entreprises. Il existe par ailleurs des lois de protection des informations sur un plan national et international. Ces lois sont bien entendu utiles, mais ne peuvent malheureusement être appliquées qu'une fois le préjudice subi !

1 Introduction

Depuis une dizaine d'années, le concept d'intelligence économique n'a cessé de prendre sa place dans les entreprises françaises, et les publications sur le sujet sont innombrables. En France, c'est surtout l'apparition du Rapport "Martre" en 1994, qui a permis à l'intelligence économique de sortir au grand jour. D'ailleurs, de nombreux auteurs sur ce concept en France, donnent la définition de l'intelligence économique proposée dans ce rapport. Cependant, si on parle beaucoup d'intelligence économique, on parle plus rarement de contre-intelligence économique. Pourtant, d'après l'étude de Bournois et Romani (2000), 95% des dirigeants estiment être en guerre économique. Cette guerre ne se fait plus entre Etats, mais entre grandes entreprises (61,5%) en raison de leur mondialisation. Dans ce contexte, il nous semble primordial d'évoquer l'importance de la sûreté économique. Baumard (1991) estime que l'on peut toujours émettre l'hypothèse qu'il existe un lieu, à un moment donné, où l'information pourra être exploitée. Il serait peut-être rationnel de ne divulguer aucune information, et de les conserver toutes, mais nous savons très bien que nous ne pouvons conserver toutes les informations par manque de place, et que nous sommes obligés de divulguer des informations lorsque l'on accomplit un acte commercial. Le meilleur exemple pour illustrer la nécessité de la sûreté économique, est sans aucun doute le cas des alliances et des partenariats, que les groupes contractent de plus en plus, dans le but d'acquérir un avantage compétitif technologique ou géographique, etc. Dans ce cas, les partenaires ont tendance à baisser leur garde, et sous prétexte qu'ils sont alliés, ils sont plus facilement prêt à partager un savoir-faire technologique, voire des équipes et des compétences. Ce partage d'informations, et ces interactions entre équipes, entraînent un risque que les deux parties négligent [17]. Or, d'après Bournois et Romani (2000), 50% des entreprises questionnées ont subi au moins une attaque[1], et ce sur le plan national ou international. Ces attaques ne concernent pas uniquement des attaques dus à l'espionnage industriel, mais aussi aux actions d'intelligence économique de la part des différentes parties. Il est vrai que l'intelligence économique doit revêtir un caractère plus légal que l'espionnage industriel, mais Guichardaz et al. (1999) évoquent au moins quatre points de convergence entre l'espionnage industriel et l'intelligence économique. Selon ces auteurs, **les champs d'application des deux pratiques sont similaires**, l'espionnage s'intéressant désormais aux aspects économiques de l'entreprise, et ayant de moins en moins une connotation militaire. La deuxième convergence concerne **le mode de récolte des informations, ainsi que le mode de traitement de ces informations**. Le troisième point concerne **l'intelligence économique qui va évoluer progressivement vers l'espionnage, le caractère offensif de l'intelligence économique va se renforcer**. Enfin, bien que l'on souhaite affirmer que les activités des services de l'espionnage relèvent de l'illégalité, **certaines activités telle que l'écoute des conversations dans les lieux publics, est tout à fait légale**. De même, l'exploitation de sources ouvertes constitue l'une des principales activités d'un service de renseignement.

Pour toutes ces raisons, nous considérons que l'intelligence économique peut être aussi dangereuse que l'espionnage industriel. Dans cette perspective, la sûreté économique demeure indispensable dans une entreprise, même si les actions de protection et/ou le fonctionnement d'un service responsable pour la protection contre la malveillance au sein d'un établissement est pour ainsi dire exclusivement réactif alors qu'il devrait surtout être préventif. Nous présenterons ainsi, le concept d'intelligence économique dans la première partie, et puis dans la deuxième partie, nous présenterons les stratégies de contre-intelligence économique qu'on appellera parfois sûreté.

2 le concept d'intelligence économique : définition et spécificités.

Bien que l'intelligence économique soit une pratique nouvelle en France, le concept ne l'est pas pour autant. Fille légitime du renseignement, l'intelligence économique fait désormais partie des premiers soucis stratégiques des entreprises du XXIème siècle. L'abondance de la littérature sur ce concept en est la preuve. Notre objectif n'étant pas de présenter une revue de littérature sur le sujet, nous nous

[1] Tous types d'attaques confondus

limiterons à présenter les définitions qui nous ont semblé les plus pertinentes, et qui nous serviront de base à la justification de l'importance de la sûreté économique.

2.1 définition(s)

Afin de présenter au mieux le concept d'intelligence économique, nous nous sommes intéressé en premier lieu à la composition du terme intelligence économique, c'est à dire intelligence d'un côté et économique de l'autre. Le terme "intelligence"[2] viendrait de l'anglais et signifie renseignement. En effet, le service de renseignement de la Reine d'Angleterre porte le nom "Intelligence". "Competitive Intelligence" est l'équivalent anglais de l'intelligence économique. En France, le concept d'intelligence économique est désigné par plusieurs termes [9]. On peut en effet rencontrer les termes *veille stratégique, information critique, gestion stratégique de l'information, surveillance concurrentielle, compétitivité et sécurité économique*. Cette sémantique assez variée prouve que l'intelligence économique ne fait pas encore tout à fait partie de la culture française!
Ceci dit, selon *Stenius* (1977) et Le Bon (2000), c'est à Luhn (1958) que nous devons la définition la plus ancienne d'un système d'intelligence économique. D'après ce dernier, "tout système de communication servant à la conduite des affaires, au sens large, peut être considéré comme un système d'intelligence. La notion d'intelligence peut être définie, dans un sens général, comme la capacité à appréhender les interrelations entre des faits disponibles de manière à guider l'action vers un but désiré". *Wilensky* (1967), a proposé une définition de l'intelligence organisationnelle qui a influencé les conceptualisations actuelles de l'intelligence économique. Cette définition est traduite ainsi : "l'intelligence organisationnelle traite du problème de la collecte, du traitement, de l'interprétation et de la communication de l'information technique et politique nécessaire au processus de prise de décision". Depuis, les définitions de l'intelligence économique accompagnent l'abondance de la littérature sur le sujet. En France, c'est la définition du *commissariat général du plan* (1994) qui a eu le plus de succès, et fut reprise par plusieurs auteurs : Bloch (1996); Martinet et Marti (1995); Jakobiak (1998); Achard et Bernat (1997); Siérès (1997). Cette définition se résume ainsi: **"l'intelligence économique est l'ensemble des actions coordonnées de recherche, de traitement, de distribution et de protection de l'information obtenue légalement et utile aux acteurs économiques en vue de la mise en œuvre de leurs stratégies individuelles et collectives".** Harbulot qui participait à la réflexion du commissariat général du plan, utilisait depuis 1992, le concept d'intelligence économique dans *La machine de guerre économique.* Il lui donne la définition suivante : "l'intelligence économique est la recherche et l'interprétation systématique de l'information accessible à tous, dans un objectif de connaissance des intentions et des capacités des acteurs. Elle englobe toutes les opérations de surveillance de l'environnement concurrentiel (protection, veille, influence)". Depuis, de nombreux auteurs ont proposé des définitions différentes mais complémentaires du concept : Rouach (1996), Besson et al. (1996) *Bruffaert-Thomas et Bouchard* (1996), *Allain-Dupré et Duhard* (1997) L'AFDIE[3], *Marcon* (1998), *Dénécé* (1998), *Lallemand* (1999), *Coulon* (1999), *Guichardaz et al.* (1999), La *SCIP*[4].
De leur côté*, Bournois et Romani* (2000) proposent une définition de l'intelligence économique et stratégique qui émane de leur recherche auprès de plusieurs dirigeants. Cette définition est la suivante: **"une démarche organisée, au service du management stratégique de l'entreprise visant à améliorer sa compétitivité par la collecte, le traitement d'informations et la diffusion de connaissances utiles à la maîtrise de son environnement (menaces et opportunités) : ce processus d'aide à la décision utilise des outils spécifiques, mobilise les salariés, et s'appuie sur l'animation de réseaux internes et externes"**. Cette définition nous semble correspondre à la réalité de la pratique de l'intelligence économique au sein des entreprises françaises. Par conséquent, nous l'adopterons pour la suite de l'article en complément de la définition de Harbulot cité plus haut.

[2] Le site "géoscopie" définit le mot *intelligence* comme "s'informer, comprendre, anticiper pour agir", alors que le mot *économie,* évoque la "production et l'utilisation de biens et services associés à l'environnement socio-politique déterminant".

[3] Association française pour le développement de l'intelligence économique, créée en octobre 1996.

[4] Society of Competitive Intelligence Professionals, c'est une association à but non lucratif. Elle publie en ligne le "competitive intelligence review et le competitive intelligence magazine". www.scip.org.ci/faq/html

Maintenant que le concept d'intelligence économique est bien défini, et dans le but de dissocier l'intelligence économique des différentes pratiques ou termes adoptés en France pour la désigner, nous présentons dans le tableau suivant les définitions des différents termes concernés.

2.2 Différence entre intelligence économique, renseignement, veille, benchmarking et lobbying.

Tableau 1. Distinction entre intelligence économique, renseignement, veille, lobbying, et benchmarking

Pratique	Définition	Département concerné
Intelligence économique [7]	C'est une démarche organisée, au service du management stratégique de l'entreprise visant à améliorer sa compétitivité par la collecte, le traitement d'informations et la diffusion de connaissances utiles à la maîtrise de son environnement (menaces et opportunités) : ce processus d'aide à la décision utilise des outils spécifiques, mobilise les salariés, et s'appuie sur l'animation de réseaux internes et externes.	Marketing/R&D/ Industriel
Renseignement économique [10]	Le renseignement d'intérêt économique recouvre l'ensemble des processus de recueil, de recherche, de traitement et de diffusion des informations destinées à l'action d'un Etat au profit d'opérateurs économiques. Le RIE se nourrit d'informations et de renseignements politiques, économiques, commerciaux, techniques, financiers, militaires et culturels utilisés à des fins économiques.	L'Etat
Renseignement [5]	C'est une valeur ajoutée à une ou plusieurs informations. C'est une connaissance élaborée, évaluée, vérifiée, recoupée et analysée. Devenu vérité, c'est un savoir **confidentiel** qui n'est pas accessible à tous. Orienté vers la prévision, il permet aux décideurs d'agir à bon escient.	En général tous les départements de l'entreprise. Le renseignement reste cependant à connotation militaire.
Veille [29]	La veille est un processus interactif, permanent et adaptatif. Il concerne les opérations de surveillance d'un marché, des évolutions en matière de technologie. Son objectif est d'acquérir la meilleure connaissance de l'environnement global de l'entreprise, afin d'optimiser les prises de décision. **"La veille est un outil primordial dans le processus d'élaboration d'une démarche d'intelligence économique"**	Tous les départements de l'entreprise
Benchmarking [31]	Le benchmarking est un processus continu d'évaluation des produits, services et méthodes par rapport à ceux des concurrents les plus sérieux ou des entreprises reconnues comme Leaders.	Marketing
Lobbying [33]	Le terme lobbying vient de Grande Bretagne. Il y a plus d'un siècle, le lobby désignait le groupe d'intérêt qui cherchait à influencer les décisions du parlement. Un peu après, les Etats Unis apprivoisent le lobbying et le réglementent.	Stratégie

2.3 Les pratiques de l'intelligence économique

La maîtrise des risques qu'une entreprise peut courir, et leur prévention, sont au cœur des finalités de la mise en œuvre des dispositifs d'intelligence économique et stratégique. Dans ce sens, Bournois et Romani (2000) évoquent trois sortes de pratiques concernant l'intelligence économique: les pratiques

offensives (légales et illégales), les pratiques défensives (spécifiques et permanentes) et les pratiques courantes. **Les pratiques défensives** peuvent exister en réaction à une attaque ciblée sur le court terme ou en protection d'intérêt pour le moyen / long terme. On peut citer parmi ces pratiques : le changement régulier des mots de passe, l'insertion de clauses de confidentialité dans les contrats avec les partenaires ou avec les cadres, etc. **Les pratiques courantes** visent à optimiser la compétitivité de l'entreprise (recouper des données sur les concurrents, limiter la circulation d'informations sensibles aux acteurs concernés, etc.). Les **pratiques offensives** consistent à concevoir et à mettre en place des manœuvres pour récupérer, exploiter ou faire circuler des informations qui vont nuire directement ou indirectement aux concurrents, par exemple. Parmi ces pratiques, on peut distinguer les *pratiques légales* qui consistent par exemple à faire parler des fournisseurs, débaucher des compétences-clés chez les concurrents, etc., et les *pratiques illégales,* comme par exemple la pose de microphones, les tentatives de concussion, le vol de plans ou de formules de produits, etc. [18].

Par ailleurs, l'étude réalisée par Bournois et Romani (2000), présente d'autres pratiques offensives cernées par les différents responsables d'intelligence économique interrogés. Nous citons *le lobbying* et l'influence évoqués par 31% de la population, ces pratiques sont apparemment celles qui viennent en première position parmi les pratiques offensives. *La désinformation* serait aussi une pratique importante et malveillante vis à vis de la concurrence. Massé et Thibaut (2001) définissent la désinformation comme "une production finalisée, destinée à exercer une influence sur le comportement des utilisateurs". Selon eux, cette pratique dépasse les pratiques de l'intelligence économique et ils la considèrent comme une technique de guerre économique. En effet, pour plusieurs auteurs (Massé et Thibaut , 2001; Kauffer, 1999, Duclos et Gustave, 1997; Bournois et Romani, 2000; Guichardaz et al., 1999), l'information est une arme de guerre redoutable. La désinformation passe par le canal des rumeurs[5][17]. Nous signalons qu'avec l'arrivée d'internet les rumeurs se déplacent plutôt de clavier à clavier! Par ailleurs, plusieurs auteurs distinguent la désinformation de la mésinformation. La désinformation peut prendre différentes formes : fausses confidences à un journaliste par exemple, saturation informationnelle (dépôts de multiples brevets dans le but de cacher la vraie nouveauté ou augmenter le temps nécessaire pour la découvrir), effets d'annonce : technologiques ou stratégiques (négociation en cours sur des partenariats, des alliances) afin de retarder les décisions de consommation ou d'accélérer celles des concurrents en les obligeant à courir plus vite : stratégie dite d'essouflement [30]. Les anglo-saxons différencient *la mésinformation* de *la désinformation* en considérant la première pratique comme une fausse information involontaire, sans l'intention de tromper, alors que dans le cas de la désinformation, l'intention de tromper est dominante. Quant à Massé et Thibaut (2001), ils définissent la mésinformation comme "un état dont la responsabilité appartient aux utilisateurs et non plus aux offreurs, par sélection d'une mauvaise information ou par une mauvaise utilisation de celle-ci. La difficulté est alors celle d'une organisation qui contrôle la qualité et la maîtrise du cycle de valorisation de l'information". L'information se trouve apparemment au cœur des pratiques de l'intelligence économique. La partie qui suit présente les informations utiles pour l'intelligence économique.

2.4 Les informations utiles pour l'intelligence économique

Bonnivard (1998), distingue trois types d'informations utiles aux acteurs de l'entreprise. Ces informations sont classées selon leur degré de complexité et de rareté.

1. **les informations publiques** : ce qu'on appelle aussi, informations ouvertes, car elles sont libres d'accès et d'exploitation, par exemple les banques de données, les publications scientifiques ou économiques, etc. A ce stade, **l'intelligence économique est qualifiée de "primaire" ou "secondaire"[6].**

[5] Les rumeurs se définissent comme des "propositions liées aux événements du jour, destinées à être crues, colportées de personne en personne, d'habitude par le bouche à oreille, sans qu'il existe de données concrètes permettant de témoigner de leur exactitude" [23].

[6] En se référant à la classification de Martre (1994), il existe quatre niveaux d'information:

- Le premier niveau est dit *primaire* : dans ce cas l'accessibilité à l'information est plus grande et la rareté est faible.

- Un deuxième niveau dit *secondaire* où l'accessibilité de l'information est de faible difficulté et la rareté est moyenne.

- Un troisième niveau dit *tactique ou de terrain* dont l'accessibilité est difficile et la rareté importante.

2. **Les informations réservées** : toutes les informations ayant un accès plus difficile. C'est le cas des brevets, des droits d'auteurs, etc. En effet, pour exploiter ce type d'informations, on est soumis à l'autorisation du titulaire du droit. Appartiennent aussi à ce niveau d'informations, les interviews, les indiscrétions, les écoutes, les informations privées qu'un concurrent mettra maladroitement dans le domaine public à l'occasion d'un salon professionnel, de rencontres, etc. A ce stade, **l'intelligence économique est qualifiée de "tactique".**
3. **Les informations confidentielles**. C'est le cas des informations protégées par le secret. On peut citer par exemple : les secrets de fabrication, les secrets commerciaux tels que : les commissions accordées aux distributeurs, les études de marchés. Le recueil de ces informations est particulièrement délicat. A ce stade, **l'intelligence économique est qualifiée de "stratégique ou de puissance"**.

Suite aux deux dernières parties, nous constatons que l'intelligence économique peut être une pratique offensive, elle peut aussi collecter des informations confidentielles. Dans ce sens, les entreprises se trouvent dans l'obligation de se protéger des pratiques d'intelligence économique de ses partenaires ou concurrents. D'après Dupré (1997), toute information ciblée implique une protection adaptée. La protection de l'information doit être adoptée tout au long de la chaîne documentaire traditionnelle. L'intelligence économique constitue un bon outil de lutte contre l'illégalité économique notamment contre l'espionnage industriel. La notion de sûreté économique trouve dans ce cas tout son sens. En revanche, et bien que tous les auteurs sur l'intelligence économique déclarent que le rôle de la protection est attribué à l'intelligence économique, nous considérons au contraire, que la protection du patrimoine (informationnel ou autre) de l'entreprise est une action bien distincte et doit être prise au sérieux au sein des entreprises. La partie qui suit nous présente le revers de l'intelligence économique, en l'occurrence la sûreté économique, et les différents outils adoptés ou à adopter par les entreprises, afin de se prémunir contre les risques associés à l'intelligence économique des différents acteurs sur le marché.

3 De l'intelligence économique à la sûreté économique

En France, on néglige ou on ne maîtrise pas la sécurité et la confidentialité des informations [34]. Cette négligence est démontrée par l'appellation attribuée par les différents auteurs au concept de sûreté. En effet, les différents auteurs désignent la sûreté par sécurité. De plus, d'après notre recherche sur le sujet, la sécurité économique concerne la sécurité sur un plan économique national, et non au niveau de l'entreprise. Geiben et Nasset (1998) différencient la sûreté de la sécurité. D'après ces auteurs, **la sécurité** concerne les mesures de prévention et de réaction mises en œuvre pour faire face à une situation d'exposition résultant **de risques accidentels**, qu'ils soient le fait de l'homme, de la machine ou de la nature. **La sûreté** concerne les mesures de prévention et de réaction mises en œuvre pour faire face à une situation d'exposition résultant de **menaces ou d'actions malveillantes**. On peut résumer cette différence par le fait que **la sécurité traite l'accidentel, la sûreté l'intentionnel.**

3.1 Les différents modes de protection, et les outils de sûreté

Il est vrai que les risques que courent les entreprises sont très importants, mais l'information considérée comme "grise" ou "noire", c'est à dire les informations stratégiques à protéger absolument ne constituent que 10% du total des informations qu'une entreprise possède. En effet, d'après plusieurs auteurs sur l'intelligence économique, les informations dites ouvertes ou blanches constituent 90% du total des informations disponibles[7]. Afin de sauvegarder le trésor de l'entreprise constitué de 10% du total de son actif, il existe plusieurs méthodes qui permettent d'assurer la sauvegarde du patrimoine de l'entreprise, notamment par le biais de l'information elle-même en l'utilisant soit comme un bouclier,

---

- Un quatrième niveau dit de *puissance ou stratégique* dont l'accessibilité est sophistiquée et délicate et la rareté très grande.

[7] Dans ce cas, la difficulté de la collecte des informations ne provient plus du secret qui l'entoure, mais de la capacité du collecteur à trier à grande échelle et de manière systématique les données disponibles (pour éviter la désinformation liée à la surinformation) et de la nécessité d'accéder à l'information stratégique dans les délais les plus courts [38].

soit comme une arme, ou par d'autres moyens transposés de la stratégie militaire telle que la classification de l'information par exemple.
Bournois et Romani (2000), distinguent deux types de protection adoptés par les entreprises qu'ils ont interrogées : **la protection intense** et **la protection de simple vigilance**.
La protection intense correspond:

- à une pratique aiguë du dépôt de brevets;
- à l'existence de procédures contraignantes de sécurité de l'information;
- à l'utilisation de systèmes intelligents sur l'internet.

La protection de simple vigilance correspond:

- à une pratique peu développée du dépôt de brevets;
- à une sécurité de l'information exempte de procédures;
- à une présence sur l'Internet au titre de la veille permanente.

Sur un plan plus technique, Massé et Thibaut (2001) distinguent quatre types de protection à envisager :

- *protection mécanique* : contrôle des accès,
- *protection humaine* : interne et externe: infiltration, faux stagiaires…
- *protection juridique* : confidentialité, propriété intellectuelle, brevets, clause de non concurrence.
- *protection logique* : sécurité informatique.

A notre avis, ces quatre types de protection sont interdépendants. Pour que la protection soit optimale, les entreprises doivent appliquer les quatre types de protection en même temps. Quant à la protection juridique, elle constitue le mode de protection le plus simple à appliquer. En effet, en cas d'attaque ultérieure ou de comportement déloyal, l'entreprise peut demander réparation de préjudice auprès du tribunal, à condition bien sûr, qu'elle ait signé avec son partenaire auparavant, un contrat ou un document juridique qui condamne un comportement déloyal de la part et d'autre des deux partenaires. Bien que cette démarche soit préventive, la réparation du préjudice vient après qu'il ait été subi. En revanche, il existe d'autres moyens de protection sur le plan juridique, comme le dépôt de brevets, marques et droits d'auteurs. Nous nous limiterons à la présentation du brevet, qui en lui seul, constitue un instrument de droit et un instrument de défense.

3.1.1 Le brevet

Le brevet est un titre de propriété. Il concerne toute invention nouvelle non évidente applicable à l'industrie. Une fois déposé, l'Etat garantit au détenteur du brevet **le monopole d'exploitation pour une durée limitée**. Son avantage, c'est que s'il est attaqué ou contourné, un brevet est défendu devant un tribunal. Son inconvénient, c'est que sa durée de vie est limitée dans le temps. Ainsi, au bout de 20 ans, un brevet tombe dans la propriété publique. Malgré tout, le brevet peut être considéré comme un instrument de défense, dans la mesure où il peut être une arme de dissuasion [36]. Il est une mini-loi, plus conçue comme un ensemble d'interdictions que comme une liste d'autorisations. C'est dans cet esprit qu'il doit empêcher les concurrents de le contourner. Enfin, nous pouvons considérer le brevet comme un instrument de management. Il peut avoir comme objectif d'influencer l'adversaire, dans la mesure où le brevet lui permet de gagner du temps et de mettre au point les processus de développement du produit en question.
En France, très peu d'entreprises déposent des brevets, bien que selon Salaün (1998), plusieurs centaines d'arrestations aient lieu chaque année pour espionnage industriel, ce qui devrait inciter les entreprises françaises à se protéger beaucoup plus. Les chiffres donnés par Bournois et Romani (2000) à cet effet sont parlants : 14% des entreprises ne déposent jamais de brevets, 25% des entreprises adoptent systématiquement les brevets, 20% des entreprises déposent très souvent des brevets (20%) contre 15% qui déposent souvent des brevets , et enfin, 16% des entreprises déposent parfois des brevets (16%).
D'après Bournois et Romani (2000), la disparité des réponses est due au fait que les entreprises aient subi des attaques majeures ou pas. En effet, ce phénomène incite les entreprises à mener une politique de dépôts de brevets systématique : 46% des entreprises qui ont identifié plusieurs attaques majeures et 39% de celles qui ont identifié une attaque majeure déposent systématiquement des brevets.

Bien que le brevet soit un mode de protection efficace, il reste avant tout un document de droit. Il faut donc savoir bien écrire un tel document. Dans les grands groupes, ce sont leurs services juridiques qui s'en occupent. Pour les PME, il est très important de s'adresser à un spécialiste en propriété industrielle pour s'en occuper. Si l'on regarde les chiffres, nous pouvons remarquer que ce sont toujours les groupes qui se soucient plus d'assurer leur protection. D'après Bournois et Romani, (2000), 85% des responsables intelligence économique[8] des grands groupes, contre 55,5% de ceux des PME, déclarent que leur connaissance juridique est suffisante pour la pratique de leur métier. En effet, les enjeux ne sont pas identiques pour un groupe à concurrence mondiale, et pour une PME à concurrence nationale. Comme nous le constatons, le brevet constitue un outil de sûreté primordial, mais heureusement, il n'est pas le seul. Il existe d'autres outils qui peuvent participer à l'instauration de la sûreté, et permettre de contourner les risques, nous traitons de ces outils dans la partie suivante.

3.1.2 La cryptologie

La cryptologie ou la cryptographie font partie de ce qu'on appelle le chiffrement. Guichardaz et al. (1999) donnent la définition suivante au chiffrement. "Le chiffrement regroupe l'ensemble des mécanismes, basés sur des techniques mathématiques, qui ont pour objet de garantir la sécurité des informations et des transactions". Les problèmes mathématiques qui servent de base à la cryptographie sont très difficiles à résoudre si l'on ne connaît pas la clé ou l'algorithme secret qui protège les informations. L'article 28 de la loi du 29 décembre 1990 définit les prestations de cryptologie, comme visant à "transformer à l'aide de conventions secrètes des informations ou signaux clairs en informations ou signaux intelligibles pour des tiers, ou à réaliser l'opération inverse, grâce à des moyens, matériels ou logiciels conçus à cet effet". Cette définition ne signifie pas que la cryptologie est entièrement sûre. D'après Guichardaz et al. (1999), la cryptographie correspond à quatre besoins de sécurité :

- le besoin d'intégrité des données qui consiste à vérifier que ces données n'ont pas été altérées accidentellement ou frauduleusement;
- le besoin d'authentification est rempli par l'identification des partenaires de l'opération et par celle de l'origine des informations.
- le besoin de non-répudiation qui s'applique à la fois à l'origine de l'information et à la réception de l'information.
- le besoin de confidentialité consiste à rendre la lecture de l'information intelligible à des tiers non autorisés lors de la conservation ou du transfert de cette information.

Malgré ses avantages, cette pratique reste encore faiblement adoptée par les entreprises. Seulement 30% des entreprises l'adoptent. C'est le secteur bancaire qui est le plus important utilisateur de cryptologie (41%), le secteur de la chimie la pratique à hauteur de 33% [7].

3.1.3 Classification de l'information

D'après Bournois et Romani (2000), 83% des entreprises dont le chiffre d'affaires est supérieur à 50 milliards de francs ont mis en place un tel système, contre 50% environ des entreprises dont le chiffre d'affaires est inférieur à 50 milliards de francs, l'ont introduit et surtout dans les entreprises dont la concurrence est mondiale (61%). Ces chiffres sont éloquents, dans la mesure où ils démontrent que seules les entreprises dont les enjeux sont importants adoptent cet outil de protection. Quelques auteurs seulement évoquent cet aspect pourtant très pragmatique.

Nous présenterons la classification évoquée par Masset et Thibaut (2001) car nous la trouvons plus complète que celle présentée par Martre (1994). D'après ces auteurs, l'information peut être classifiée[9] selon son processus d'acquisition ou selon la liberté d'accès. selon la première classification, on peut rencontrer *l'information texte* : information structurée dans une documentation; *floue*: acquise par des contacts humains; *experte* : acquise en interne ou en externe auprès des consultants; *foire* : acquise dans des contextes de rassemblement. suivant la deuxième classification, on peut rencontrer

---

[8] Nous rappelons que la plupart des auteurs considèrent la sûreté comme faisant partie des objectifs de l'intelligence économique.

[9] Nous avons repris deux formes uniquement de classification de l'information évoquées par Massé et Thibaut (2001), alors qu'ils en proposent quatre. Les deux autre classifications, étant selon le rôle joué, ou selon le mode d'appropriation. Ces deux classifications ne pouvant jouer un rôle dans le cadre du portage.

l'information dite *blanche* à laquelle tout le monde peut accéder librement; *grise* : non commercialisée mais accessible si on sait la rechercher; *noire* : secrète, non accessible sauf par le moyen de l'espionnage industriel. Ce sont **l'information grise et l'information noire que les entreprises sont censées protéger** surtout dans le cadre du portage, où la présence du partenaire à l'intérieur des locaux peut lui faciliter la tâche.
En ce qui concerne la **classification**, du point de vue légal, nous tenons à préciser que l'article 4-5 du décret n°81-514 du 12 mai 1981, en cours de refonte, établit les règles de protection des secrets de l'Etat. Ce décret exige que les informations soient "classifiées". Ces informations sont ainsi réparties en trois catégories: **très secret défense**[10]**, secret défense et confidentiel défense**, suivant leur niveau de confidentialité. L'accès à ces informations est réglementé : il faut posséder une autorisation préalable délivrée à la suite d'une procédure "d'habilitation"[11], et avoir, de surcroît, "besoin d'en connaître" pour l'accomplissement de sa fonction ou de sa mission [14]. La classification de l'information présente un intérêt majeur, dans la mesure où elle peut prévenir les risques d'espionnage en restreignant la diffusion des informations classées aux personnes concernées. Cependant, il reste à se protéger ou se défendre du risque de désinformation. Dans ce cas, on peut avoir recours à ce qu'on appelle la contre-information. Nous présentons cet aspect dans la partie qui suit.

3.2 Comment se protéger de la guerre de l'information

D'après Guichardaz et al. (1999), il existe quatre stratégies de contre-espionnage regroupées en quatre catégories, selon le champ de menaces et celui auquel elles s'appliquent.
La *première stratégie* s'applique à **l'individu**. En effet, chaque personne est censée protéger les informations qu'il détient. Ces informations peuvent être d'ordre personnel ou en relation avec son entreprise. La *deuxième stratégie* s'applique à un **département ou un service** de l'entreprise (le département marketing par exemple). Il s'agit de protéger des informations détenues par un petit groupe de personnes. La *troisième stratégie* concerne un champ plus large, celui de **l'entreprise** en tant qu'institution. Dans ce cas, l'entreprise formalise les pratiques de protection et les contre-mesures. La *quatrième stratégie* concerne **le groupe**, c'est à dire tout le réseau de l'entreprise : filiales, sous-traitants, etc.

3.2.1 L'individu et la protection

Le coeur de toute protection est l'individu. Chaque personne travaillant au sein d'une entreprise est concernée par la protection du patrimoine de l'entreprise. Malheureusement, comme le rappelle Markus Wolf dans ses mémoires, "il y a toujours des personnes qui parlent trop, en dépit de toutes les mises en garde". Nous pensons en effet, que la protection des informations doit rentrer dans le cadre de l'éducation civique des individus, sans pour autant tomber dans la paranoïa. Il est important dans ce cadre, de classifier les informations, afin de mieux protéger les informations confidentielles. Pour cette raison, afin d'assurer la sûreté optimale d'une entreprise en général, et d'un groupe porteur en particulier, il convient de définir une stratégie de protection institutionnelle afin de sensibiliser tous les membres de l'institution, et de veiller ainsi aux intérêts du groupe.

3.2.2 L'entreprise et la protection

Selon Guichardaz et al.(1999), pour définir sa stratégie de protection, il convient de se poser quatre questions fondamentales : *comment est collectée l'information?; comment est protégée l'information?* dans un sens où l'on doit prendre comme base les trois grands risques qui menacent l'information : sa destruction, sa modification ou sa compromission; *comment est-elle gérée l'information au quotidien?* (ou sont les informations et qui les détient); *comment l'information est-elle transportée?* (depuis le point de collecte jusqu'au point de stockage), par exemple d'une filiale au siège.

[10] *Très secret-défense* : informations dont la divulgation est de nature à nuire à la défense nationale et à la sûreté de l'Etat et qui concernent les priorités gouvernementales en matière de défense.
Secret défense : informations dont la divulgation est de nature à nuire à la défense nationale et à la sûreté de l'Etat.
Confidentiel défense : informations qui ne présentent pas en elles-mêmes un caractère secret mais dont la connaissance, la réunion, ou l'exploitation peuvent conduire à la divulgation d'un secret intéressant la défense nationale et la sûreté de l'Etat.
[11] Les habilitations sont effectuées par la DPSD (direction de protection et de sécurité de la défense).

Dans le cadre du fonctionnement normal d'une entreprise, le partenaire ou le concurrent, peut trouver une faille dans le circuit d'information de l'entreprise, et influencer le détenteur des informations stratégiques afin d'obtenir les informations qu'il souhaite, etc. l'approche de contre-intelligence économique doit donc porter sur plusieurs points : les recrutements, la sensibilisation et la formation, les clauses de non-concurrence, la protection des informations stratégiques, la protection des documents électroniques et des locaux, la gestion de projets, la messagerie électronique.

3.2.3 La contre-information

La contre-information peut être définie comme "l'ensemble des actions de communication qui, grâce à une information pertinente et vérifiable, permettent d'atténuer, d'annuler ou de retourner contre son instigateur une attaque par l'information" [21].
Le grand principe de la contre-information est d'exploiter les contradictions de l'adversaire. Ceci dit, il existe plusieurs critères d'efficacité de la contre-information. D'après Harbulot et Jacques-Gustave (1998), ces critères sont les suivants :
- Pour être crédible, la contre-information s'attache à véhiculer de l'information ouverte ou argumentée, non manipulée, donc facilement vérifiable;
- Où, quand, comment et dans quelles proportions diffuser l'information? La contre-information est affaire de stratégie et de management de l'information;
- Il s'agit d'attaquer systématiquement les contradictions et les points faibles de l'adversaire;
- L'argumentaire d'attaque est d'autant plus incisif si l'évidence des faits relatés est établie;
- La communication est liée à l'exemplarité de la démonstration et à une utilisation habile des caisses de résonance spontanées.

Nous constatons qu'il existe plusieurs moyens de protection de l'information. Pour optimiser l'adoption de ces moyens, il conviendrait à notre avis de faire appel à une personne, qui a la capacité de jouer le rôle de chef d'orchestre, afin d'assurer une harmonie dans l'utilisation de ces moyens, et ce entre les différents services concernés, et instaurer ainsi un règlement intérieur de sûreté, qui doit être appliqué par tout le groupe et ses filiales.

3.3 Sécurité de l'information et légalité

Une protection spécifique des secrets industriels et commerciaux contre l'espionnage a été à plusieurs reprises menée par différentes organisations internationales afin d'endiguer ces pratiques jugées inacceptables. Nous citons ainsi :
OMPI art.54 de la loi modèle — LICCD (Ligue Internationale contre la concurrence déloyale) " Violation des secrets industriels et commerciaux en matière concurrentielle " (Congrès Vienne 1969, Genève 1972, Rome 1974, Munich 1976) — Conseil de l'Europe, 1) Rapport sur " les problèmes juridiques liés à l'espionnage industriel " : Doc. 2897, 20 janvier 1971 et Doc. 3440, 14 mai 1974, 2) " Aspects criminologiques de la délinquance d'affaires et criminalité dans le domaine de l'informatique ", Publication Strasbourg, novembre 1976, 3) " Rapport final d'activité sur la criminalité en relation avec l'ordinateur ", 1989-OCDE, 1) " Étude sur le phénomène de la fraude informatique : analyse de la politique juridique de la zone de l'OCDE ", 1984, 2) " La fraude liée à l'informatique : analyse des politiques juridiques ", PICC, n°10, 1986 (Dasquié, 1999).
Sur le plan national, il existe aussi plusieurs lois concernant la protection des secrets, la cryptologie, mais aussi contre le sabotage informatique. Ne pouvant pas tout présenter, nous recommandons de se référer à Dasquié (1999), et Warusfel (1995) qui présentent les différentes lois concernant la protection de l'information ou du secret.

4 Conclusion

Cet article nous a présenté le concept d'intelligence économique et ses différentes pratiques. Ces pratiques sont aussi bien offensives que défensives. Les entreprises, notamment les plus grandes, se trouvent alors dans l'obligation de protéger leurs patrimoines scientifiques et technologiques, des pratiques offensives des différents acteurs. L'information semble être à la fois, l'arme et le bouclier de cette guerre économique, appelée aussi guerre d'information.
Bien que toutes les entreprises ne soient pas conscientes des dangers des pratiques d'intelligence économique des différentes parties sur le marché, la notion de sûreté économique existe et doit être

dissociée de l'intelligence économique. Les pratiques de la sûreté doivent concerner toutes les actions et mesures de protection. Ces mesures de protection peuvent être considérées sur un plan juridique (brevet, clauses de confidentialités, clauses de non-concurrence, ainsi que toutes les lois concernant la protection du secret). Sur le plan technique, les entreprises peuvent avoir recours à la cryptologie, la classification de l'information, et toutes les techniques de contre-information adoptées sur le plan de la communication. Enfin, sur le plan informatique, il existe aussi plusieurs techniques de protection, mais nous n'avons pas pu traiter ces aspects dans cet article.

Bibliographie

[1.] ACHARD P. et BERNAT J.P, *L'intelligence économique : mode d'emploi*, ADBS, 1998.
[2.] ALLAIN-DUPRE P. et DUHARD N., *Les armes secrètes de la décision : la gestion de l'information au service de la performance économique*", Gualino éditeur, 1997.
[3.] BAUMARD P., *Stratégie et surveillance des environnements concurrentiels*, Masson, 1991.
[4.] BERNAT J.P., *L'intelligence économique dans une grande entreprise*, Cahiers de MARS, N°162, 1999, pp.145-157.
[5.] BESSON B. et POSSIN J.C., *Du renseignement à l'intelligence économique*, Dunod, 1996.
[6.] BLOCH A., *L'intelligence économique*, Economica, Collection Economie Poche, N°38, 1996.
[7.] BOURNOIS et ROMANI, *L'intelligence économique et stratégique dans les entreprises françaises*, Economica, 2000.
[8.] COULON G., *L'intelligence économique : une culture*, Cahiers de MARS, N°162, 1999 pp.174-179.
[9.] DASQUIE Guillaume, *Secrètes affaires, les services secrets infiltrent les entreprises*, Flammarion, 1999.
[10.] DENECE E. a, *Le renseignement d'intérêt économique*, Veille, N°14, 1998, pp.19-21.
[11.] DENECE E. b, *Intelligence économique et renseignement*, Défense Nationale, N°1, 1998, pp. 48-58.
[12.] DENECE E., *Intelligence concurrentielle et renseignement d'intérêt économique : complémentarité de l'action des entreprises et des Etats*, Cahiers de MARS, N°162, 1999, pp.133-144.
[13.] DENECE E., *Intelligence économique et renseignement*, Renseignement et opérations spéciales, N°5, 2000, pp. 137-147.
[14.] DUPONT de DINECHIN Y. et QUINIO L., *La protection du patrimoine scientifique et technique*, Administration, N°180, 1998, pp. 47-50.
[15.] DUPRE J., *Intelligence économique : les ambiguïtés de la protection des intérêts économiques nationaux*, Droit et Défense, N°3, 1997, pp. 58-64.
[16.] GEIBEN B., NASSET J.J., *Sécurité, Sûreté : la gestion intégrée des risques dans les organisations*, Editions d'organisation, 1998.
[17.] GUICHARDAZ P. et al., *L'infoguerre : stratégies de contre-intelligence économique*, Dunod, 1999.
[18.] HARBULOT C., *Techniques offensives et guerre économique*, Revue Politique et Parlementaire, N°948, juillet 1990, pp. 614-72.
[19.] HARBULOT C. *La machine de guerre économique*, Economica, 1992.
[20.] HARBULOT C., *Intelligence économique et guerre de l'information*, Cahiers de MARS, N°162, 1999 pp.102-107.
[21.] HARBULOT C. et JACQUES-GUSTAVE P., *Manœuvre médiatique et compétition économique*, Enjeux Atlantiques, N°16, 1998 pp. 16-19.
[22.] JAKOBIAK F., *L'intelligence économique en pratique*, Editions d'Organisation, 2001.
[23.] KAPFERER J.N., *Rumeurs, le plus vieux média du monde*, Editions du seuil, 1987.
[24.] KAUFFER R., *L'arme de la désinformation-les multinationales américaines en guerre contre l'Europe*, Grasset, 1999.
[25.] LALLEMAND, *La défense économique*, Cahiers de MARS, N°162, 1999, pp.116-123.
[26.] LE BON J., *De l'intelligence économique à la veille Marketing et commerciale: vers une nécessaire mise au point conceptuelle et théorique*, Papier de Recherche ESSEC, mai 2000.

[27.] MARCON C., *Intelligence économique : l'environnement pertinent comme variable stratégique . justification théorique et approche instrumentale*, Thèse de Doctorat Es Sciences Economiques, Poitiers, 1998.
[28.] MARTRE H., *La prise de conscience de l'importance de l'intelligence économique*, Les Cahiers de MARS, N°162, 1999, pp. 70-74.
[29.] MARTRE H., *Rapport du groupe, intelligence économique et stratégie des entreprises*, commissariat général du plan, documentation française, 1994.
[30.] MASSE G., THIBAUT F., *Intelligence économique, un guide pour une économie de l'intelligence*, De Boeck Universités, 2001.
[31.] PICHOT-DUCLOS et GUSTAVE J., *La guerre pour, contre et par l'information*, Objectif Défense, N°62, mars 1997, pp.92-94.
[32.] ROMAGNI P., *Le Benchmarking*, in 10 outils clés du management, les éditions du GO, 1996.
[33.] ROMAGNI P. et al., *L'intelligence économique au service de la stratégie d'entreprise ou l'information comme outil de gestion*, PUF, 1997.
[34.] ROMAGNI P. et al., *L'intelligence économique au service de l'entreprise*, Les Presses du Management, 1998.
[35.] ROUACH et al., *La veille technologique et l'intelligence économique*, PUF, 1996.
[36.] SALAÜN C., *Guerre économique et propriété industrielle*", Défense Nationale, août 1998, pp. 111-117.
[37.] SIERES J. et FRICAUD-CHAGNAUD C-G., *Les Armes et la Toge. Mélanges offerts à André Martel : Penser la défense. Informatique, information et intelligence économique. Défense, problèmes de l'heure. Consensus français, consensus européen*, Centre d'Histoire Militaire et d'Etudes de Défense Nationale de Montpellier, 1997, pp. 229-243.
[38.] WARUSSFEL B., *Secret et propriété industrielle*, Droit et Défense, N°2, 1995, pp.74-77.